PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-338798
(43)Date of publication of application : 10.12.1999

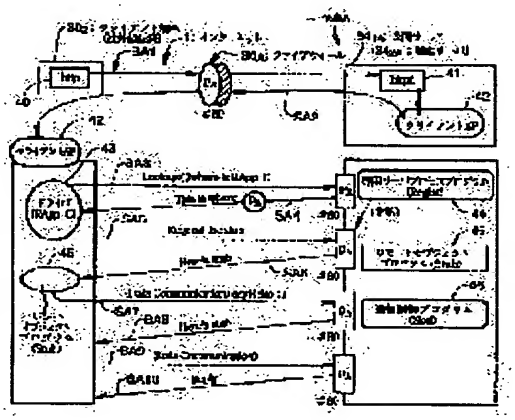
(51)Int.CI. G06F 13/00
// H04L 9/08

(21)Application number : 10-146372
(22)Date of filing : 27.05.1998

(71)Applicant : NTT COMMUNICATION WARE KK
(72)Inventor : NAGAOKA TORU
SAKATA MASAFUMI
KOBAYASHI KAZUE

(54) NETWORK SYSTEM AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a computer readable recording medium recording a network system program without requiring an original security dedicated port for the security setting of a fire wall.
SOLUTION: This system is provided with a certified client terminal 302 and a secret server 342A connected through a fire wall 35A0 to an internet 1, and an http 40 from the client terminal 302 is inputted through a port PA of a port number #80 to the secret server 342A. After a specified client application program(AP) 42 is downloaded to the client terminal 302, the secret server 342A reports the information of the port PA to use a protocol sequence to the client terminal 302. Afterwards, data communication is performed between the client terminal 302 and the secret server 342A through the internet 1 and the port PA by a dedicated protocol.



LEGAL STATUS

[Date of request for examination] 23.03.2001
[Date of sending the examiner's decision of rejection] 13.07.2004
[Kind of final disposal of application other than the examiner's decision of

rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－338798

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｈ
			３５１Ｚ
// Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ

審査請求　未請求　請求項の数５　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－146372

(22)出願日　平成10年(1998)５月27日

(71)出願人　397065480
エヌ・ティ・ティ・コミュニケーションウェア株式会社
東京都港区港南一丁目９番１号

(72)発明者　長岡　亨
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内

(72)発明者　坂田　雅史
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内

(74)代理人　弁理士　志賀　正武　（外２名）

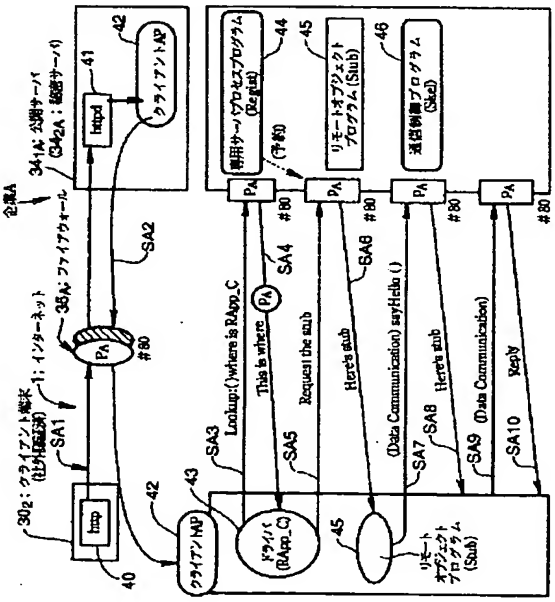
最終頁に続く

(54)【発明の名称】　ネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムプログラムを記録したコンピュータ読み取り可能な記録媒体を得ること。

【解決手段】　本発明は、認証済のクライアント端末３０２と、ファイアウォール３５Ａを介してインターネット１に接続された秘密サーバ３４２Ａとを備え、クライアント端末３０２からのｈｔｔｐ４０は、ポート番号＃８０のポートＰＡを通過して秘密サーバ３４２Ａに入力される。秘密サーバ３４２Ａは特定のクライアントＡＰ（アプリケーションプログラム）４２をクライアント端末３０２にダウンロードした後、プロトコルシーケンスを使用するポートｐＡの情報をクライアント端末３０２に通知する。以後専用のプロトコルによりインターネット１およびポートｐＡを介してクライアント端末３０２と秘密サーバ３４２Ａとの間でデータ通信が行われる。



1

【特許請求の範囲】

【請求項１】　ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、

前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うことを特徴とするネットワークシステム。

【請求項２】　ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第１のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第１のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第２のポートとして設定し、

前記プロキシサーバは、前記クライアント端末から見たポートを前記第１のポートから前記第２のポートに変換する一方、前記サーバから見たポートを前記第２のポートから前記第１のポートに変換し、

前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うことを特徴とするネットワークシステム。

【請求項３】　前記クライアント端末に設けられ、前記データ通信におけるデータの暗号化および復号化を行う第１の暗号化通信制御部と、

前記サーバに設けられ、前記データ通信におけるデータの暗号化および復号化を行う第２の暗号化通信制御部と、

2

を具備することを特徴とする請求項１または２に記載のネットワークシステム。

【請求項４】　ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、

前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５】　ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、

前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第１のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第１のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第２のポートとして設定し、

前記プロキシサーバは、前記クライアント端末から見たポートを前記第１のポートから前記第２のポートに変換する一方、前記サーバから見たポートを前記第２のポートから前記第１のポートに変換し、

前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアント端末

からネットワークを介してサーバへのアクセスに用いられるネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】従来より、企業内におけるＬＡＮ（ローカルエリアネットワーク）環境においては、基幹業務に必要な多種多様なプロトコルが使用されているため、ＬＡＮ等のシステムをインターネットを介して接続することは、後述するファイアウォールにおけるプロトコルの通過の可否等の問題から困難であった。しかしながら、近時、分散コンピューティング技術の浸透、Ｊａｖａの普及により、インターネットを介して企業間ＬＡＮ等のシステムを接続することによりネットワークシステムを構築することが可能になっている。ここで、このようなネットワークシステムを構築する場合には、ファイアウォールを設置することにより、セキュリティを確保している。

【０００３】ここで、ファイアウォールとは、情報システムの本体とインターネットとの結合部分に設けられ、防火壁の役割を持つシステムであって、権限のない者の不正侵入の防止、コンピュータ・ウィルスの防止を行うものをいう。また、上述したファイアウォールを有するネットワークシステムにおいては、この環境下で使用できるプロトコル種別に対して、セキュリティポリシーに沿った制限を課すことにより、任意のプロトコルを通過させないことにより、セキュリティを確保している。

【０００４】図５は、上述した従来のネットワークシステムの概略構成を示す図である。この図において、１は、複数のネットワークが互いに接続されてなるインターネットであり、図５に示す例では、インターネット１は、企業ＡのＬＡＮと企業ＢのＬＡＮとを接続している。企業Ａにおいて、２は、各種のデータベースを記憶部に保持するデータベースサーバであり、ファイアウォール３を介してインターネット１に接続されている。

【０００５】このデータベースサーバ２に対しては、認証された端末のみがファイアウォール３を介してアクセスすることができる。一方、未認証の端末は、ファイアウォール３を通過してデータベースサーバ２にアクセスできないようになっている。４は、インターネット１に接続された公開ＷＷＷ（World Wide Web）サーバであり、認証、未認証を問わずいずれの端末であってもアクセス可能とされている。

【０００６】一方、企業Ｂにおいて、５は、各種データベースを記憶部に保持するデータベースサーバであり、ファイアウォール６を介してインターネット１に接続されている。このデータベースサーバ５に対しては、認証された端末のみがファイアウォール６を介してアクセスすることができる。７は、インターネット１に接続された公開ＷＷＷサーバであり、認証、未認証を問わずいずれの端末であってもアクセス可能とされている。８は、ファイアウォール６を介してインターネット１に接続された社内ＷＷＷサーバであり、この社内ＷＷＷサーバ８に対しては、認証された端末のみがファイアウォール６を介してアクセスすることができる。

【０００７】図６は、従来のネットワークシステムにおける主要部の構成を示す図である。この図において、９は、クライアント側に設置されたクライアント端末であり、インターネット１に接続されている。このクライアント端末９は、インターネット１を介して後述するＷＷＷサーバ１３およびデータベースサーバ１９へアクセスするものである。

【０００８】クライアント端末９において、１０は、クライアント端末９により実行されるクライアントアプリケーションプログラムであり、通信制御、暗号化制御、プロトコル制御等を行うためのプログラムである。また、クライアントアプリケーションプログラム１０は、クライアント端末９からインターネット１を介して他の企業側のアプリケーションを利用するときに実行されるプログラムである。１１は、暗号化通信制御部であり、予め定義された特定のプロトコルサービスポートを通過するデータグラムに対して、データ属性を問わず、暗号化、復号化を行うための暗号化専用プロトコルを制御する機能（例えば、ＳＳＬ：Secure SocketLayer）を有している。１２はセッションを管理するセッション管理部である。

【０００９】ＷＷＷサーバ１３は、ファイアウォール１４を介してインターネット１に接続されており、クライアント端末９からの起動を契機として機能する端末である。ここで、ファイアウォール１４には、複数のポートが設けられており、このポートとしては、未認証のクライアント端末９からのプロトコルを通す通常のポートと、認証済みのクライアント端末９からのプロトコルのみを通すセキュリティ通信用のポートに大別される。

【００１０】上記ＷＷＷサーバ１３において、１５は、上述した暗号化通信制御部１１と同様の機能を有する暗号化通信制御部である。１６は、セッションを管理するセッション管理部である。１７は、ＷＷＷサーバ１３により実行されるサーバアプリケーションプログラムであり、クライアント端末９との間の通信制御等に用いられる。１８は、後述するデータベース２０に対するアクセス制御を行うＤＢ（データベース）通信制御部である。データベースサーバ１９は、記憶部にデータベース２０を保持するものである。

【００１１】ここで、図６に示すネットワークシステムの動作について、図７（ａ）および（ｂ）に示す動作説明図を用いて説明する。図７（ａ）は、未認証の社外のクライアント端末９１からのアクセス動作を説明する図であり、図７（ｂ）は、未認証および認証済みのクライアント端末９１および９２からのアクセス動作を説明する図である。

【００１２】ここで、図７（ａ）および（ｂ）において、クライアント端末９１は、図６に示す、未認証の一のクライアント端末９に対応しており、社外に設置されている。クライアント端末９２は、図６に示す、認証済の他のクライアント端末９に対応しており、社外に設置されている。

【００１３】図７（ａ）および（ｂ）に示すファイアウォール１４は、ポートＰAおよびポートＰBを有しており、このポートＰAは、ポート番号として＃８０が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。従って、上記ポートＰAのポート番号＃８０は、公知である。一方、ポートＰBは、ポート番号としてポート番号＃Ｘが付与されており、認証済みのクライアント端末９２からのアクセスのために設定されているポートである。従って、ポートＰBのポート番号＃Ｘは、認証済のクライアント端末９２のクライアントのみが通信に利用することができる番号である。言い換えれば、ポートＰBには、特定のクライアント端末９２からのみしかアクセスできない。

【００１４】図７（ａ）および（ｂ）に示す公開サーバ１３１および秘密サーバ１３２は、図６に示すＷＷＷサーバ１３に対応している。ここで、公開サーバ１３１には、インターネット１、ファイアウォール１４のポートＰAを介して、例えば、クライアント端末９１がアクセスする。一方、秘密サーバ１３２には、インターネット１、１４のポートＰBを介して、例えば、クライアント端末９２がアクセスする。２１は、社内に設置されたクライアント端末であり、ファイアウォール１４の内側におけるセキュリティが確保されているため、直接、公開サーバ１３１および秘密サーバ１３２へアクセス可能である。

【００１５】図７（ａ）において、未認証のクライアント端末９１は、通常、ファイアウォール１４のポートＰAを通過して公開サーバ１３１へｈｔｔｐ（Hyper Text Transfer Protocol）を用いてアクセスする。このとき、上記ｈｔｔｐは、ポートＰAを通過することができる。ここで、クライアント端末９１から秘密サーバ１３２へのアクセスしようとした場合には、クライアント端末９１のクライアントがポートＰBのポート番号＃Ｘを知らないため、ファイアウォール１４を通過することができない。言い換えれば、クライアント端末９１からのｈｔｔｐは、ポートＰBを通過することができないため、クライアント端末９１と秘密サーバ１３２との間で通信が成立しないのである。従って、この場合には、クライアント端末９１が秘密サーバ１３２へアクセスすることができないため、セキュリティが確保される。

【００１６】一方、図７（ｂ）において、クライアント端末９２から秘密サーバ１３２へアクセスしようとした場合には、クライアント端末９２は、セキュリティ通信専用のプロトコルを用いて、まず、ポートＰBへアクセスする。このとき、上記プロトコルがポートＰBを通過することができるので、クライアント端末９２は、秘密サーバ１３２へアクセスできる。

【００１７】

【発明が解決しようとする課題】ところで、上述した従来のネットワークシステムにおいては、ファイアウォールを用いた、よりセキュアな企業間通信を実現することが、強いニーズとなっている。しかしながら、上述したネットワークシステムのファイアウォール環境においては、階層的に分散された組織分散型のファイアウォールが多段構成で存在するため、１つの新しいプロトコルをファイアウォールを通過させるために、多大なる準備、運用稼働が必要となるという問題があった。この準備、運用稼働としては、図６に示すファイアウォールのポートの再設定、クライアントアプリケーションプログラム１０、サーバアプリケーションプログラム１７の仕様変更等が挙げられる。

【００１８】ここで、図８を参照して、従来のネットワークシステムの問題点について詳述する。図８において、図７（ａ）および（ｂ）に対応する部分には、同一の符号を付ける。図８に示す企業Ａにおいて、１４Ａは、図７に示すファイアウォール１４と同様の機能を有するファイアウォールであり、インターネット１（図６参照）と公開サーバ１３１Aおよび秘密サーバ１３２Aとの間に設けられている。ここで、ファイアウォール１４Ａは、ポートＰAおよびポートＰCを有している。

【００１９】上記ポートＰAは、ポート番号として＃８０が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。一方、ポートＰCは、ポート番号としてポート番号＃Ｙが付与されており、認証済みのクライアント端末９２からのアクセス（分散コンピューティング通信）のために設定されているポートである。このポートＰCは、セキュリティ専用ポートである。　従って、ポートＰCのポート番号＃Ｙは、認証済のクライアント端末９２のクライアントのみが通信に利用することができる番号である。言い換えれば、ポートＰCには、特定のクライアント端末９２からのみしかアクセスできない。２１Aは、企業Ａ内に設置されたクライアント端末であり、公開サーバ１３１Aおよび秘密サーバ１３２Aへアクセスする。

【００２０】また、企業Ｂにおいて、１４Bは、インターネット１と秘密サーバ１３２Bとの間に設けられたファイアウォールであり、共に分散コンピューティング通信専用のポートＰCおよびポートＰDを有している。上記ポートＰCには、ポート番号＃としてＹが、ポートＰDには、ポート番号＃としてＺが各々付与されている。ポートＰCのポート番号＃Ｙは、認証済のクライアント端末９２のクライアントのみが通信に利用することができる番号である。これらのポートＰCおよびＰDは、セキュリ

ティ専用ポートである。

【００２１】上記構成において、未認証のクライアント端末９１は、通常、ファイアウォール１４ＡのポートＰＡを通過して公開サーバ１３１Ａへｈｔｔｐ（Hyper Text Transfer Protocol）を用いてアクセスする。このとき、上記ｈｔｔｐは、ポートＰＡを通過することができる。なお、クライアント端末９１は、上述した動作と同様にして、ファイアウォール１４ＡのポートＰＣ、およびファイアウォール１４ＢのポートＰＣ、ＰＤを通過して当該サーバへアクセスできない。

【００２２】一方、クライアント端末９２から秘密サーバ１３２Ａへアクセスしようとした場合には、クライアント端末９２は、セキュリティ通信専用のプロトコルを用いて、まず、ファイアウォール１４ＡのポートＰＣへアクセスする。このとき、上記プロトコルがポートＰＣを通過することができるので、クライアント端末９２は、秘密サーバ１３２Ａへアクセスできる。

【００２３】ここで、ファイアウォール１４Ｂが既に他のサービスプロトコルのために割り当て済みである状態で、クライアント端末９２がファイアウォール１４ＢのポートＰＣを介して秘密サーバ１３２Ｂへアクセスした場合について説明する。この場合には、ポートＰＣがふさがっているため、ファイアウォール１４Ｂにおいては、ポートＰＤを設定する必要がある。このポート設定の変更の情報は、クライアント端末９２の管理者に通知される必要がある。ここで、クライアント端末９２には、複数のファイアウォールにおけるポート設定情報を管理するポート管理部２２が設けられている。

【００２４】ここで、従来のネットワークシステム（図８参照）においては、分散コンピューティングを実現するために、必要とする全ての機能（サーバアプリケーション）が存在する全ての相手先システム（他企業内システム）に対してクライアント端末９２等からのアクセスを可能とすべく、すべてのセキュリティポリシを満足するためのセキュリティ制御が行われている。しかしながら、図８を参照して説明したように、従来のネットワークシステムにおいては、ポート設定変更のルールが企業によってまちまちであり、ポート管理部２２への定義情報の管理が煩雑化するとともに、その制御が複雑になってしまう。従って、このようなポート設定の条件を加味して、業務単位に対応付けてアプリケーションの実行を行うためには、非常に複雑な実装方式を検討・開発せざるを得えない。特に、セキュリティ案件に関わる実装変更については、企業単位に重要かつ慎重な検討課題であり、これが早急なシステム実現への妨げになっている。本発明はこのような背景の下になされたもので、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムおよびプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００２５】

【課題を解決するための手段】請求項１に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うことを特徴とする。また、請求項２に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第１のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第１のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第２のポートとして設定し、前記プロキシサーバは、前記クライアント端末から見たポートを前記第１のポートから前記第２のポートに変換する一方、前記サーバから見たポートを前記第２のポートから前記第１のポートに変換し、前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うことを特徴とする。また、請求項３に記載の発明は、請求項１または２に記載のネットワークシステムにおいて、前記クライアント端末に設けられ、前記データ通信におけるデータの暗号化および復号化を行う第１の暗号化通信制御部と、前記サーバに設けられ、前記データ通信におけるデータの暗号化および復号化を行う第２の暗号化通信制御部とを具備することを特徴とする。また、請求項４に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールとを備え、

前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号のポートを介して、前記クライアント端末へダウンロードし、前記クライアント端末と前記サーバアクセスとは、前記プログラムを実行して、前記専用プロトコルにより、前記ネットワークおよび前記公知のポート番号のポートを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。また、請求項５に記載の発明は、ネットワークに接続された認証済のクライアント端末と、前記ネットワークに接続されたサーバと、前記サーバと前記ネットワークに介挿されたファイアウォールと、前記ファイアウォールにおけるポート変換を行うプロキシサーバとを備え、前記クライアント端末は、前記ファイアウォールにおける公知のポート番号のポートを介して公知のプロトコルにより前記サーバへアクセスし、前記サーバは、アクセスしてきた前記クライアント端末が認証済のものである場合、該クライアント端末と自身との間のみで有効な専用プロトコルを実現するためのプログラムを前記公知のポート番号の第１のポートを介して、前記クライアント端末へダウンロードした後、前記クライアント端末に対して前記第１のポートを通信用のポートとして通知するとともに、自身が使用するポートを前記公知のポート番号以外のポート番号の第２のポートとして設定し、前記プロキシサーバは、前記クライアント端末から見たポートを前記第１のポートから前記第２のポートに変換する一方、前記サーバから見たポートを前記第２のポートから前記第１のポートに変換し、前記クライアント端末と前記サーバとは、前記プログラムを実行して、前記専用のプロトコルにより、前記ネットワーク、前記ファイアウォールおよび前記プロキシサーバを介してデータ通信を行うこととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００２６】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。図１は本発明の一実施形態によるネットワークシステムにおける主要部の構成を示す図である。この図において、図６の各部に対応する部分には同一の符号を付ける。図１に示す３０は、クライアント側に設置されたクライアント端末であり、インターネット１に接続されている。このクライアント端末３０は、インターネット１を介して後述するＷＷＷサーバ３４およびデータベースサーバ１９へアクセスするものである。

【００２７】クライアント端末３０において、３１は、クライアント端末３０により実行されるクライアントアプリケーションプログラムであり、通信制御、暗号化制御、プロトコル制御等を行うためのプログラムである。また、クライアントアプリケーションプログラム１０は、後述する専用のプロトコルを用いるときに実行されるとともに、クライアント端末３０からインターネット１およびファイアウォール３５を介して他の企業側のアプリケーションを利用するときに実行されるプログラムである。

【００２８】３２は、分散コンピューティング通信制御部であり、後述するサーバアプリケーションプログラム３８の一部を動的にクライアントアプリケーションプログラム３１と関連づけたり、複製したりする。また、分散コンピューティング通信制御部３２は、上記サーバアプリケーションプログラム３８の一部をあたかもクライアント端末３０に既存の業務アプリケーションプログラムのように扱えるような実行環境を実現するための、通信プロトコル機能を有している。３３は、暗号化通信制御部であり、図６に示す暗号化通信制御部１１と同一の機能を有している。

【００２９】ＷＷＷサーバ３４は、ファイアウォール３５を介してインターネット１に接続されており、クライアント端末３０からの起動を契機として機能する端末である。このファイアウォール３５には、複数のポートが設定されているが、クライアント端末３０が未認証であるか認証済であるかを問わず、クライアント端末３０とＷＷＷサーバ３４との間の通信においては、ポート番号＃８０のポートが用いられる。このポート番号＃８０のポートは、公知であり、ｈｔｔｐ等の一般的なプロトコルを通過させるためのものである。このファイアウォール３５のポート設定状況および、クライアント端末３０とＷＷＷサーバ３４との間の通信プロトコルの詳細については後述する。

【００３０】上記ＷＷＷサーバ３４において、３６は、上述した暗号化通信制御部１１と同様の機能を有する暗号化通信制御部である。３７は、上述した分散コンピューティング通信制御部３２と同様の機能を有する分散コンピューティング通信制御部である。３８は、ＷＷＷサーバ３４により実行されるサーバアプリケーションプログラムであり、クライアント端末３０との間の通信制御等に用いられる。また、サーバアプリケーションプログラム３８は、後述する専用のプロトコルを用いる場合に実行されるプログラムである。３９は、データベース２０に対するアクセス制御を行うＤＢ（データベース）通信制御部である。

【００３１】ここで、図１に示すネットワークシステムを企業間における分散コンピューティング通信に適用した場合の構成について図２を参照して説明する。図２に示すネットワークシステムは、企業Ａ内のシステムと企業Ｂ内のシステムとがインターネット１（図１参照）を

介して接続されており、かつ該インターネット１には、未認証のクライアント端末３０１および認証済のクライアント端末３０２が接続されている。

【００３２】ここで、図２に示すクライアント端末３０１は、図１に示す、未認証の一のクライアント端末３０に対応しており、社外に設置されている。クライアント端末３０２は、図１に示す、認証済の他のクライアント端末３０に対応しており、社外に設置されている。ここで、クライアント端末３０１および３０２の各記憶部には図１に示すクライアントアプリケーションプログラム３１が記憶されている。

【００３３】企業Ａにおいて、ファイアウォール３５Ａは、図１に示すファイアウォール３５に対応しており、ポートＰＡを有している。このポートＰＡは、ポート番号として＃８０が付与されており、不特定多数のクライアント端末からのアクセスのために設定されているポートである。なお、実際には、ファイアウォール３５Ａには、論理的なポートが複数設けられており、それぞれのポートのポート番号は、任意に設定される。ただし、以下の説明において、用いられるポートは、ポート番号＃８０のもののみである。

【００３４】３４１Ａは、図１に示すＷＷＷサーバ３４に対応する公開サーバであり、インターネット１およびファイアウォール３５Ａを介してクライアント端末３０１によりアクセスされる。３４２Ａは、図１に示すＷＷＷサーバ３４に対応する秘密サーバであり、後述する専用のプロトコルにより、インターネット１およびファイアウォール３５Ａ（ポートＰＡ）を介して認証済のクライアント端末３０２によりアクセスされる。ここで、公開サーバ３４１Ａおよび秘密サーバ３４２Ｂの各記憶部には、図１に示すサーバアプリケーションプログラム３８が記憶されている。クライアント端末２１Ａは、企業Ａ内に設けられており、公開サーバ３４１Ａおよび秘密サーバ３４２Ａに対してアクセスする。

【００３５】一方、企業Ｂにおいて、ファイアウォール３５Ｂは、図１に示すファイアウォール３５に対応しており、ポートＰＡを有している。このポートＰＡは、ポート番号として＃８０が付与されている。このファイアウォール３５Ｂの機能は、上述したファイアウォール３５Ａの機能と同一である。３４２Ｂは、専用のプロトコルにより、インターネット１およびファイアウォール３５Ｂ（ポートＰＡ）を介して、クライアント端末３０２によりアクセスされる。この秘密サーバ３４２Ｂの記憶部には、図１に示すサーバアプリケーションプログラム３８が設けられている。クライアント端末２１Ｂは、企業Ｂ内に設けられており、秘密サーバ３４２Ｂにアクセスする。

【００３６】次に、上述した一実施形態によるネットワークシステムの動作について図３を参照して説明する。この図において、図２の各部に対応する部分には同一の符号を付けその説明を省略する。この図においては、図２に示す認証済のクライアント端末３０２がインターネット１および企業Ａ内のファイアウォール３５Ａを介して秘密サーバ３４２Ａにアクセスする例について図示されている。また、図３に示すファイアウォール３５Ａにおいては、ポートＰＡと、該ポートＰＡとは異なるポートｐＡとが備えられているが、上記ポートＰＡとポートｐＡには、いずれもポート番号＃８０が時間的にずれて付与される。すなわち、ファイアウォール３５Ａにおいては、ポート番号＃８０が付与されるポートが変化する。

【００３７】また、図３に示すクライアントアプリケーションプログラム（ＡＰ）４２は、図１に示すクライアントアプリケーションプログラム３１に相当するものであり、ドライバ（ＲＡｐｐ＿Ｃ）４３を有している。このドライバ４３は、クライアントアプリケーションプログラム４２により実現される機能の一部であり、クライアント端末３０２と秘密サーバ３４２Ａとの間のプロトコルシーケンスを制御するものである。

【００３８】また、専用サーバプロセスプログラム（Ｒｅｇｉｓｔ）４４は、サーバアプリケーションプログラム３８の一部をなすプログラムであり、秘密サーバ３４２Ａとクライアント端末３０２との間の通信制御を行うためのものである。この専用サーバプロセスプログラム４４は、リモートオブジェクトプログラム（ｓｔｕｂ）４５と通信制御プログラム（Ｓｋｅｌ）４６とから構成されている。

【００３９】このリモートオブジェクトプログラム４５は、ファイアウォール３５Ａおよびインターネット１を介してクライアント端末３０２へ転送された後、クライアント端末３０２により実行されるプログラムであり、通信制御を行うためのものである。一方、通信制御プログラム４６は、秘密サーバ３４２Ａにより実行されるプログラムであり、リモートオブジェクトプログラム４５と対をなして、通信制御を行うためのものである。

【００４０】上記構成において、秘密サーバ３４２Ａが起動されると、専用サーバプロセスプログラム４４が実行され、秘密サーバ３４２Ａは、動作可能状態とされる。この状態において、手順ＳＡ１では、クライアント端末３０２から、ｈｔｔｐ４０および認証済であることを示すクライアント認証データがファイアウォール３５Ａへインターネット１を介して送出される。今、ファイアウォール３５Ａのポート ＰＡにポート番号＃８０が付与されているものとすると、上記ｈｔｔｐ４０は、ファイアウォール３５Ａのポート ＰＡを通過して、秘密サーバ３４２Ａに入る。

【００４１】これにより、秘密サーバ３４２Ａは、クライアント端末３０２が認証済の端末であるか否かを、最初に送受される通信データの一部に含まれるクライアント認証データから判断し、サーバ側の認証に失敗したとき、以後の動作を行わない。今の場合、秘密サーバ３４２Ａは、クライアント端末３０２が認証済の端末であるた

め、ｈｔｔｐｄ（http deamon）４１により、クライアントアプリケーションプログラム４２を認識する。

【００４２】そして、手順ＳＡ２では、秘密サーバ３４２Aは、上記クライアントアプリケーションプログラム４２をポートＰAおよびインターネット１を介してクライアント端末３０２へＪａｖａ　Ａｐｐｌｅｔ等の形態をとってダウンロードする。これにより、クライアント端末３０２においては、クライアントアプリケーションプログラム４２が実行されることにより分散コンピューティン通信が開始される。

【００４３】次に、手順ＳＡ３では、クライアント端末３０２は、ドライバ４３を用いて、分散コンピューティング通信で用いるファイアウォール３５Aにおけるポート（番号）の情報をインターネット１およびポートＰAを介して秘密サーバ３４２Aへ要求する。これにより、手順ＳＡ４では、秘密サーバ３４２Aは、ポートとしてポートＰAに代えてポートｐAを予約するとともに、該ポートｐAにポート番号＃８０を付与する。すなわち、この予約により、ポート番号＃８０のポートは、ポートＰAからポートｐAに変更されたのである。以後のプロトコルシーケンスは、すべてポートｐA（ポート番号＃８０）を介して行われる。

【００４４】次に、手順ＳＡ４では、秘密サーバ３４２Aは、プロトコルシーケンスを行うポートとして予約されたポートｐA（ポート番号＃８０）の情報をポートｐAおよびインターネット１を介してクライアント端末３０２へ送出する。これにより、クライアント端末３０２は、以後に使用するファイアウォール３５AのポートがポートｐA（ポート番号＃８０）であることを認識する。

【００４５】次に、手順ＳＡ５では、秘密サーバ３４２Aは、指定されたポートｐA（ポート番号＃８０）を介しての通信に必要なリモートオブジェクトプログラム４５のダウンロードを要求するための情報をインターネット１およびポートｐAを介して秘密サーバ３４２Aへ送出する。これにより、手順ＳＡ６では、秘密サーバ３４２Aは、リモートオブジェクトプログラム４５をポートｐAおよびインターネット１を介してクライアント端末３０２へダウンロードする。

【００４６】これにより、クライアント端末３０２において、リモートオブジェクトプログラム４５が実行される。以後、手順ＳＡ７～手順ＳＡ１０のように、クライアント端末３０２と秘密サーバ３４２Aとの間では、インターネット１およびファイアウォール３５Aのポートｐを介してデータ通信が行われる。また、このデータ通信においては、図１に示す暗号化通信制御部３３、３６によりデータの暗号化、復号化が行われているので、セキュアな通信が実現できる。

【００４７】以上説明したように、上述した一実施形態によるネットワークシステムによれば、専用のプロトコルを用いることにより、ファイアウォール３５Aにおけるポートを常にポート番号＃８０のポートとするように構成したので、クライアント端末３０２におけるポート管理が不要となる。このことから、上述した一実施形態によるネットワークシステムによれば、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムを得ることができるという効果が得られる。また、上述した一実施形態によるネットワークシステムによれば、既存のイントラネットセキュリティ・ポリシに特別な設定変更を行うことなく、それまで通過を認めていなかった分散コンピューティング通信を安全に利用することができるという効果が得られる。

【００４８】また、上述した一実施形態によるネットワークシステムによれば、ファイアウォール３５Aのポートを通過させた全てのデータに対してプロトコルレベルで暗号化、復号化が施されることにより、運用的な利便性を実現することができるという効果が得られる。さらに、上述した一実施形態によるネットワークシステムによれば、企業に個々に確立されているイントラネット設計に大きな変更を加える必要がないため、関連企業間で設計検討・実装等を極めて短期間で完了させることができ、ひいてはこれらをつなぐ分散システムの構築を短期間で行うことができるという効果が得られる。

【００４９】以上本発明の一実施形態によるネットワークシステムについて詳述してきたが、具体的な構成はこの一実施形態に限られるものではなく本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、上述した一実施形態によるネットワークシステムにおいては、図３に示す構成について説明したが、これに代えて図４に示す構成のものを採用してもよい。

【００５０】以下、図４に示すネットワークシステムについて説明する。図４において、図３の各部に対応する部分には同一の符号を付けその説明を省略する。図４においては、ブロキシサーバ４７が新たに設けられている。また、図４においては、ファイアウォール３５Aは、ポート番号＃８０のポートＰAと、該ポートＰAと異なるポート番号のポートＰBとを有している。上記ポートＰBのポート番号は、例えば、＃Ｘとされている。

【００５１】ブロキシサーバ４７は、ファイアウォール３５A（または、秘密サーバ３４２A）に設けられており、企業A側のプライベートネットワークからインターネット１等のパブリックなネットワークに、またはその逆の場合に情報の通過を許可しないという役目をするサーバである。図４においては、ブロキシサーバ４７は、ポートＰAに入力された情報をポートＰBを介して秘密サーバ３４２Aへ出力する一方、ポートＰBに入力された情報をポートＰAを介してインターネット１へ出力するという、ポート変換機能を有している。すなわち、ブロキシサーバ４７により、クライアント端末３０２から秘密

サーバ３４２Aを見た場合、アクセス可能なポートがポートＰAとされる一方、秘密サーバ３４２Aから秘密サーバ３４２Aを見た場合、アクセス可能なポートがポートＰBとされる。

【００５２】上記構成において、秘密サーバ３４２Aが起動されると、専用サーバプロセスプログラム４４が実行され、秘密サーバ３４２Aは、動作可能状態とされる。この状態において、手順ＳＢ１では、クライアント端末３０２から、ｈｔｔｐ４０がファイアウォール３５Aへインターネット１を介して送出される。今、ファイアウォール３５AのポートP_Aにポート番号＃８０が付与されているものとすると、上記ｈｔｔｐ４０は、ファイアウォール３５AのポートP_Aを通過して、秘密サーバ３４２Aに入る。これにより、秘密サーバ３４２Aは、前述した動作と同様にして、ｈｔｔｐｄ４１により、クライアントアプリケーションプログラム４２を認識する。

【００５３】そして、手順ＳＢ２では、秘密サーバ３４２Aは、上記クライアントアプリケーションプログラム４２をポートP_Aおよびインターネット１を介してクライアント端末３０２へＪａｖａ　Ａｐｐｌｅｔ等の形態をとってダウンロードする。これにより、クライアント端末３０２においてはクライアントアプリケーションプログラム４２が実行されることにより分散コンピューティン通信が開始される。

【００５４】次に、手順ＳＢ３では、クライアント端末３０２は、ドライバ４３を用いて、分散コンピューティング通信で用いるファイアウォール３５Aにおけるポート（番号）の情報をインターネット１およびポートP_Aを介して秘密サーバ３４２Aへ要求する。これにより、手順ＳＢ４では、秘密サーバ３４２Aは、自身が使用するポートとして、ポートP_B（ポート番号＃Ｘ）を予約するとともに、該ポートP_B（ポート番号＃Ｘ）の情報をプロキシサーバ４７に送出する。また、秘密サーバ３４２Bは、クライアント端末３０２が使用するポートとしてポートP_A（ポート番号＃８０）の情報をポートP_Aおよびインターネット１を介してクライアント端末３０２へ送出する。

【００５５】これにより、プロキシサーバ４７においては、ポートP_A→ポートP_B（ポートP_A→ポートP_B）というポート変換が定義される。この定義により、秘密サーバ３４２Aからクライアント端末３０２を見た場合のプロトコルシーケンスが、ファイアウォール３５AのポートP_B上で行われる一方、クライアント端末３０２から秘密サーバ３４２Aを見た場合のプロトコルシーケンスは、ファイアウォール３５AのポートP_A上で行われる。つまり、秘密サーバ３４２Aは、分散コンピューティング通信を行うポートとしてポートP_Bを（ポート番号＃Ｘ）認識している一方、クライアント端末３０２は、上記ポートとしてポートP_A（ポート番号＃８０）を認識している。

【００５６】次に、手順ＳＢ５では、秘密サーバ３４２Aは、指定されたポートP_A（ポート番号＃８０）を介しての通信に必要なリモートオブジェクトプログラム４５のダウンロードを要求するための情報をインターネット１へ送出する。これにより、プロキシサーバ４７においてポート変換（ポートP_A→ポートP_B）が行われ、上記情報は、ポートP_A、ポートP_Bを介して秘密サーバ３４２Aに入力される。

【００５７】これにより、手順ＳＢ６では、秘密サーバ３４２Aは、リモートオブジェクトプログラム４５をポートP_Bを介して送出する。このとき、プロキシサーバ４７により、ポート変換（ポートP_B→ポートP_A）が行われ、上記リモートオブジェクトプログラム４５は、ポートP_B、ポートP_Aおよびインターネット１を介してクライアント端末３０２へダウンロードされる。

【００５８】これにより、クライアント端末３０２において、リモートオブジェクトプログラム４５が実行される。以後、手順ＳＢ７～手順ＳＢ１０のように、クライアント端末３０２と秘密サーバ３４２Aとの間では、インターネット１およびファイアウォール３５AのポートP_A、ポートP_Bを介してデータ通信が行われる。また、このデータ通信においては、図１に示す暗号化通信制御部３３、３６によりデータの暗号化、復号化が行われているので、セキュアな通信が実現できる。

【００５９】また、上述した一実施形態によるネットワークシステムにおいては、上述した機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するように構成してもよい。なお、ここでいうコンピュータシステムとは、ＯＳ（オペレーティングシステム）や周辺機器等のハードウェアを含むものとする。また、コンピュータシステムは、WWWシステムを利用しているものであれば、ホームページ提供環境（または表示環境）を含むものとする。

【００６０】

【発明の効果】以上説明したように、本発明によれば、専用プロトコルを用いることにより、ファイアウォールにおけるポートを常に公知のポート番号のポートとするように構成したので、クライアント端末側におけるポート管理が不要になる。このことから、本発明によれば、ファイアウォールのセキュリティ設定に独自のセキュリティ専用ポートを必要としないネットワークシステムを得ることができるという効果が得られる。また、請求項３に記載の発明によれば、第１および第２の暗号化通信制御部によりデータの暗号化、復号化が行われているので、セキュアな通信を実現できるという効果が得られる。

【図面の簡単な説明】

【図１】　本発明の一実施形態によるネットワークシス

17

テムの主要部の構成を示す図である。

【図２】　同一実施形態によるネットワークシステムを企業間における分散コンピューティング通信に適用した場合の構成を示す図である。

【図３】　同一実施形態によるネットワークシステムの動作を説明する図である。

【図４】　同他の実施形態によるネットワークシステムの構成および動作を説明する図である。

【図５】　従来のネットワークシステムの概略構成を示す図である。

【図６】　従来のネットワークシステムの主要部の構成を示す図である。

【図７】　従来のネットワークシステムの動作を説明する図である。

【図８】　従来のネットワークシステムの問題点を説明する図である。

【符号の説明】

１　インターネット

３０、３０１、３０２　クライアント端末

18

＊３１　クライアントアプリケーションプログラム

３２　分散コンピューティング通信制御部

３３　暗号化通信制御部

３４　ＷＷＷサーバ

３４1A　公開サーバ

３４2A、３４2B　秘密サーバ

３５、３５A、３５B　ファイアウォール

３６　暗号化通信制御部

３７　分散コンピューティング通信制御部

３８　サーバアプリケーションプログラム

３９　ＤＢ通信制御部

４０　ｈｔｔｐ

４２　クライアントアプリケーションプログラム

４３　ドライバ

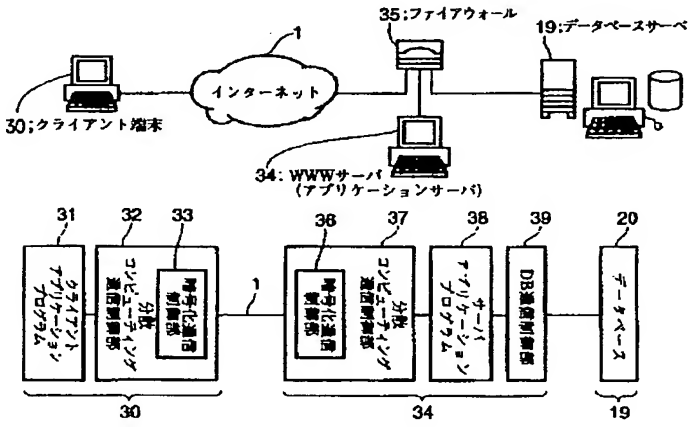
４４　専用サーバプロセスプログラム

４５　リモートオブジェクトプログラム

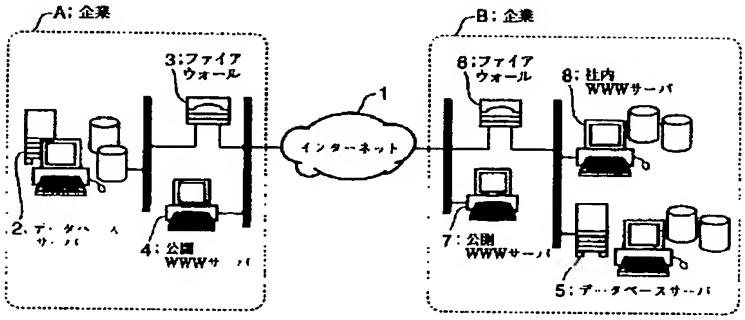
４６　通信制御プログラム

４７　プロキシサーバ

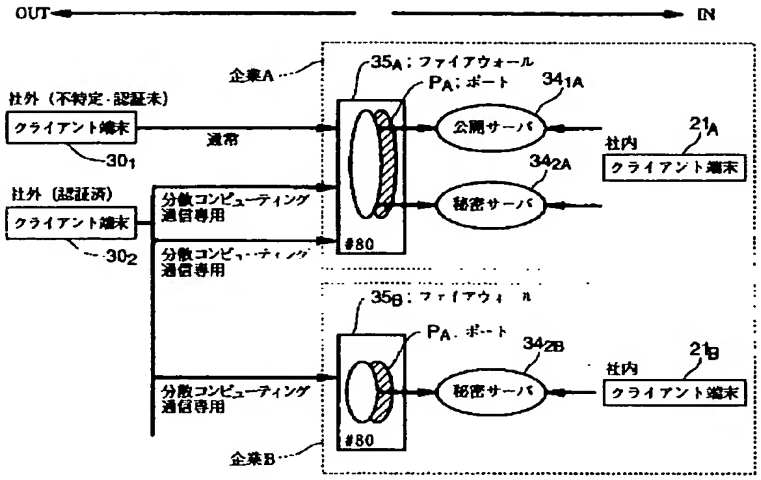
【図１】



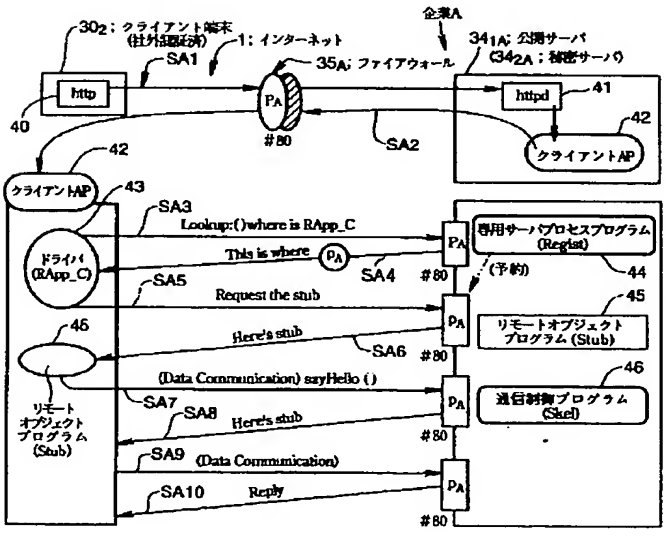
【図５】



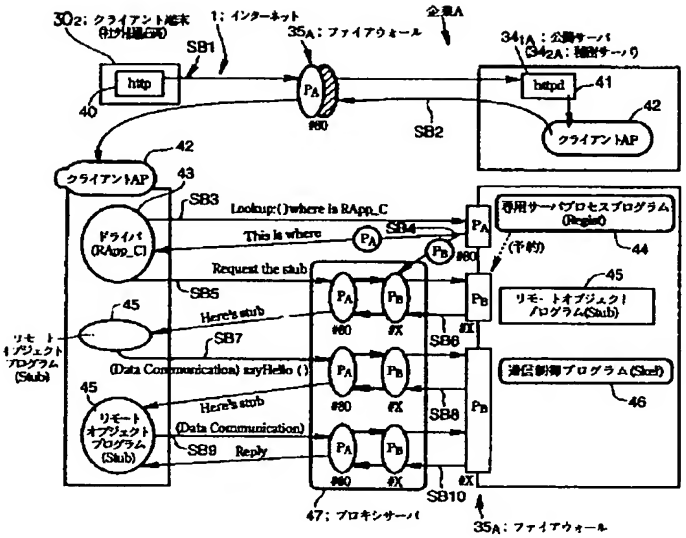
【図２】


OUT
IN
企業A
35A：ファイアウォール
PA：ポート
341A
社外（不特定・認証未）
クライアント端末
301
通常
公開サーバ
21A
社内
クライアント端末
342A
社外（認証済）
クライアント端末
302
分散コンピューティング通信専用
秘密サーバ
#80
分散コンピューティング通信専用
35B：ファイアウォール
PA：ポート
342B
21B
社内
分散コンピューティング通信専用
秘密サーバ
クライアント端末
#80
企業B

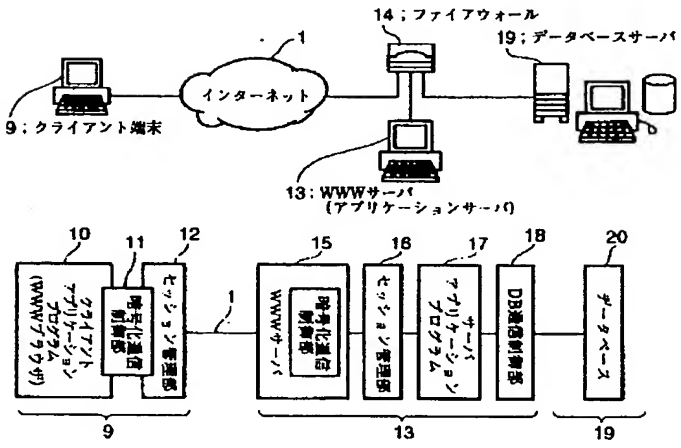
【図３】


302：クライアント端末（社外認証済）
1：インターネット
企業A
341A：公開サーバ
(342A：秘密サーバ)
SA1
35A：ファイアウォール
http
PA
#80
httpd
41
40
SA2
42
クライアントAP
42
クライアントAP
43
SA3
Lookup:()where is RApp_C
This is where
PA
SA4
#80
専用サーバプロセスプログラム (Regist)
(予約)
44
ドライバ (RApp_C)
SA5
Request the stub
PA
#80
45
リモートオブジェクトプログラム (Stub)
46
Here's stub
SA6
#80
(Data Communication) sayHello ()
PA
#80
46
通信制御プログラム (Skel)
SA7
SA8
Here's stub
リモートオブジェクトプログラム (Stub)
SA9
(Data Communication)
PA
#80
SA10
Reply

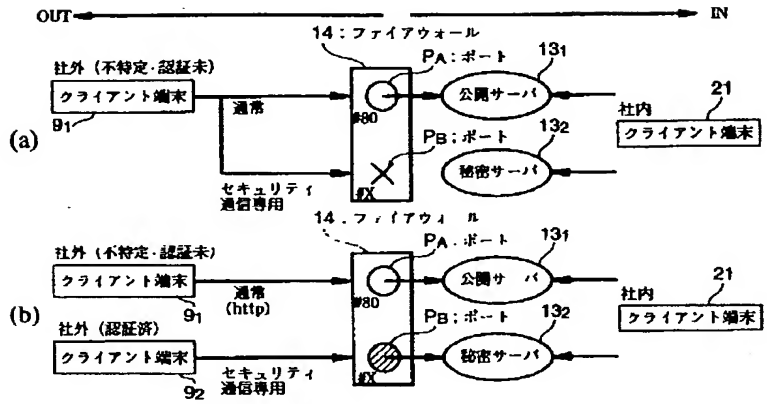
【図４】


1；インターネット
企業A
35A：ファイアウォール
SB1
http
40
PA
#80
SB2
34₁A：公開サーバ
(34₂A：秘密サーバ)
httpd
41
42
クライアントAP
43
SB3
Lookup:()where is RApp_C
This is where
SB4
ドライバ
(RApp_C)
専用サーバプロセスプログラム
(Regist)
44
(予約)
Request the stub
SB5
45
リモートオブジェクトプログラム(Stub)
Here's stub
SB7
(Data Communication) sayHello ()
#X
SB6
通信制御プログラムA(Skel)
46
SB8
Here's stub
(Data Communication)
SB9
Reply
SB10
47；プロキシサーバ
35A：ファイアウォール

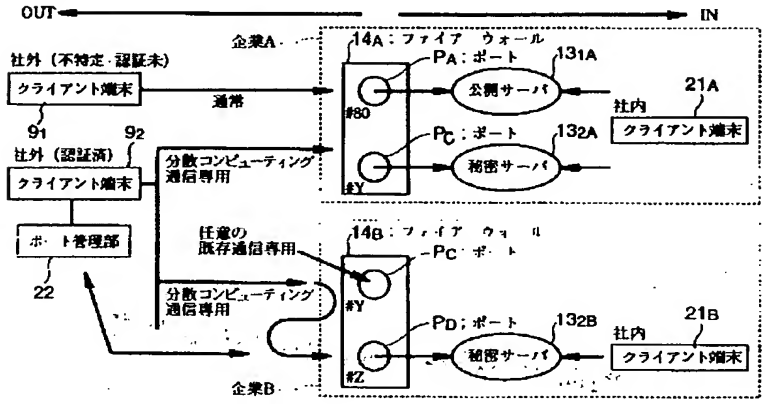
【図６】


14；ファイアウォール
19；データベースサーバ
1
インターネット
9；クライアント端末
13；WWWサーバ
(アプリケーションサーバ)
10
11
12
15
16
17
18
20
クライアントアプリケーションプログラム(WWWブラウザ)
WWWサーバ
サーバアプリケーションプログラム
DB連携制御部
データベース
9
13
19

【図７】



【図８】



フロントページの続き

(72)発明者　小林　和恵
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内

This Page Blank (uspto)